CLAIMS:

What is claimed is:

1. A method of authenticating a data processing device, comprising:

receiving an electrical signal having a data signal added therein;

extracting the data signal from the electrical signal;

comparing data of the data signal to security information stored in the data processing device; and

permitting operation of the data processing device based on the comparison of the data of the data signal to the security information.

2. The method of claim 1, wherein the operation is one of power-up and boot-up of the device.

3. The method of claim 1, further comprising:

storing a record of the data signal in a history data structure, wherein the history data structure includes a data value of the data signal and a timestamp of the data signal.

4. The method of claim 1, further comprising:

receiving a data packet from a sending device via a data network, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

comparing the second data value to the first data value; and

permitting processing of the data packet if the second data value matches the first data value.

5. The method of claim 4, further comprising:

adding an identifier of the sending device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices.

6. The method of claim 5, further comprising:

comparing an identifier of the sending device to identifiers in at least one of the list of authorized devices and the list of unauthorized devices prior to querying the history data structure;

automatically permitting the processing of the data packet if the identifier of the sending device is in the list of authorized devices; and

automatically denying processing of the data packet if the identifier of the sending device is in the list of unauthorized devices.

7. The method of claim 5, further comprising:

periodically clearing the list of authorized devices and the list of unauthorized devices.

8. The method of claim 1, further comprising:

receiving the security information from a security device associated with the data network.

9. The method of claim 1, wherein the data signal is generated based on security information from a security device associated with the data network.

10. The method of claim 1, wherein the data processing device is one of a computer, a workstation, a storage system, a peripheral device, and a portable computing device.

11. The method of claim 1, wherein the electrical signal is indicative of a location of the data processing device.

12. A computer program product in a computer readable medium for authenticating a data processing device, comprising:

first instructions for receiving an electrical signal having a data signal added therein;

second instructions for extracting the data signal from the electrical signal;

third instructions for comparing data of the data signal to security information stored in the data processing device; and

fourth instructions for permitting operation of the data processing device based on the comparison of the data of the data signal to the security information.

13. The computer program product of claim 12, wherein the operation is one of power-up and boot-up of the device.

14. The computer program product of claim 12, further comprising:

fifth instructions for storing a record of the data signal in a history data structure, wherein the history data structure includes a data value of the data signal and a timestamp of the data signal.

15. The computer program product of claim 12, further comprising:

fifth instructions for receiving a data packet from a sending device via a data network, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

sixth instructions for querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

seventh instructions for comparing the second data value to the first data value; and

eighth instructions for permitting processing of the data packet if the second data value matches the first data value.

16. The computer program product of claim 15, further comprising:

ninth instructions for adding an identifier of the sending device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices.

17. The computer program product of claim 16, further comprising:

tenth instructions for comparing an identifier of the sending device to identifiers in at least one of the list of authorized devices and the list of unauthorized devices prior to querying the history data structure;

eleventh instructions for automatically permitting the processing of the data packet if the identifier of the sending device is in the list of authorized devices; and

twelfth instructions for automatically denying processing of the data packet if the identifier of the sending device is in the list of unauthorized devices.

18. The computer program product of claim 16, further comprising:

tenth instructions for periodically clearing the list of authorized devices and the list of unauthorized devices.

19. The computer program product of claim 12, further comprising:

fifth instructions for receiving the security information from a security device associated with the data network.

20. The computer program product of claim 12, wherein the data signal is generated based on security information from a security device associated with the data network.

21. The computer program product of claim 12, wherein the data processing device is one of a computer, a workstation, a storage system, a peripheral device, and a portable computing device.

22. The computer program product of claim 12, wherein the electrical signal is indicative of a location of the data processing device.

23. An apparatus for authenticating a data processing device, comprising:

means for receiving an electrical signal having a data signal added therein;

means for extracting the data signal from the electrical signal;

means for comparing data of the data signal to security information stored in the data processing device; and

means for permitting operation of the data processing device based on the comparison of the data of the data signal to the security information.

24. A method of securing a data network, comprising:

receiving an electrical signal from an external electrical network;

adding a data signal to the electrical signal to generate a modified electrical signal, wherein the data signal includes security data;

outputting the modified electrical signal to a local electrical network; and

permitting operation of devices on a data network based on an authentication of the devices using the data signal extracted from the modified electrical signal.

25. The method of claim 24, further comprising:

receiving the modified electrical signal at a device coupled to the electrical network;

extracting the data signal from the modified electrical signal; and

authenticating an operation of the device based on the extracted data signal.

26. The method of claim 25, wherein the operation is one of power-up and boot-up of the device.

27. The method of claim 24, further comprising:

storing a record of the data signal in a history data structure associated with a device on the data network, wherein the history data structure includes a data value of the data signal and a timestamp of the data signal.

28. The method of claim 24, further comprising:

receiving a data packet from a second device, via a data network, in a first device, wherein the data packet includes a first data value and a first timestamp associated with the first data value;

querying a history data structure for a second data value associated with a second timestamp in the history data structure based on the first timestamp;

comparing the second data value to the first data value; and

permitting processing of the data packet if the second data value matches the first data value.

29. The method of claim 28, further comprising:

adding an identifier of the second device to a list based on the comparison of the second data value to the first data value, wherein if the second data value matches the first data value, the list is a list of authorized devices, and wherein if the second data value does not match the first data value, the list is a list of unauthorized devices.

30. The method of claim 29, further comprising:

comparing an identifier of the second device to identifiers in at least one of the list of authorized devices and the list of unauthorized devices prior to querying the history data structure;

automatically permitting the processing of the data packet if the identifier of the second device is in the list of authorized devices; and

automatically denying processing of the data packet if the identifier of the second device is in the list of unauthorized devices.

31. The method of claim 29, further comprising:

periodically clearing the list of authorized devices and the list of unauthorized devices.

32. The method of claim 24, further comprising:

receiving security information from a security device associated with the data network; and

generating the data signal based on the received security information.

33. The method of claim 24, wherein the devices are data processing devices that include one or more of a computer, a workstation, a storage system, a peripheral device, and a portable computing device.

34. The method of claim 24, wherein the modified electrical signal is indicative of a location of devices coupled to the local electrical network.

35. A computer program product in a computer readable medium for securing a data network, comprising:

first instructions for receiving an electrical signal from an external electrical network;

second instructions for adding a data signal to the electrical signal to generate a modified electrical signal, wherein the data signal includes security data;

third instructions for outputting the modified electrical signal to a local electrical network; and

fourth instructions for permitting operation of devices on a data network based on an authentication of the devices using the data signal extracted from the modified electrical signal.

36. A system for securing a data network, comprising:

an electrical power signal modification device coupled to an electrical network and the data network;

a server coupled to the data network; and

a data processing device coupled to both the electrical network and the data network, wherein the electrical power signal modification device receives an electrical signal from an external electrical network, adds a data signal to the electrical signal to generate a modified electrical signal, the data signal including security data generated based on security information received from the server, and outputs the modified electrical signal to a local electrical network, and wherein an operation of the data processing device is permitted based on an authentication of the data

processing device using the data signal extracted from the modified electrical signal.

37. The system of claim 36, wherein the operation is one of a power-up operation and a boot-up operation.

38. The system of claim 36, wherein the operation is processing of a data packet received from another data processing device.

39. The system of claim 36, wherein the modified electrical signal is indicative of a location of the data processing device.